IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF PENNSYLVANIA

JANE DOE, individually and on behalf of all others similarly situated,	CIVIL DIVISION
Plaintiff,	No. _____
v.	Code:_____
SAMSUNG ELECTRONICS AMERICA, INC. and SAMSUNG ELECTRONICS CO., LTD.	CLASS ACTION
Defendants.	**COMPLAINT - CLASS ACTION**

INTRODUCTION

1. Each year, an estimated 13.5 million people are victims of stalking in the United States, with nearly one in three women and one in six men experiencing stalking at some point in their lifetime.[1]

2. Stalking can manifest in a host of ways, most often through unwanted and repeated behaviors such as phone calls, texts, visits, gifts, internet posts, or any other series of acts that would cause fear in a reasonable person. Regardless of the acts the stalker employs, the common theme of stalking behavior is the fear elicited in the victim.

3. This fear undermines and erodes a victim's autonomy and drastically disrupts their day-to-day life. One in eight employed stalking victims miss time from work because of their victimization and more than half lose more than five days of work.[2] One in seven stalking victims

[1] Stalking Prevention Awareness and Resource Center (SPARC), Stalking Fact Sheet (available at: https://www.stalkingawareness.org/wp-content/uploads/2019/01/SPARC_StalkngFactSheet_2018_FINAL.pdf)

[2] Baum, K., Catalano, S., & Rand, M. (2009). Stalking Victimization in the United States. Washington, DC: Bureau of Justice Statistics (available at: https://www.justice.gov/sites/default/files/ovw/legacy/2012/08/15/bjs-stalking-rpt.pdf).

move as a result of their victimization.[3] Unsurprisingly, stalking victims suffer much higher rates of depression, anxiety, insomnia, and social dysfunction than people in the general population.[4]

4. Technology has increased the tools available to a stalker, with burner phones or call blocking software providing anonymity, and free email services and social media platforms providing a limitless vector for harassing electronic messages and posts.

5. One of the most dangerous and frightening technologies employed by stalkers is the use of real-time location information to track victims. These technologies allow stalkers to follow their victims' movements in real time and to undo any attempt on the part of the victim to evade or hide from the stalker. If one's location is constantly being transmitted to an abuser, there is no place to run.

6. One of the products that has revolutionized the scope, breadth, and ease of location-based stalking is the Samsung Galaxy SmartTag ("SmartTag"). Introduced in January 2021, this device is roughly the size of a quarter, and its sole purpose is to transmit its location to its owner. Samsung also sells the Galaxy SmartTag+ ("SmartTag+", or together with the SmartTag, the "SmartTags").

7. What separates Samsung's SmartTags from any competitor product are the unparalleled accuracy, ease of use (it fits seamlessly into Samsung's existing suite of products, known as the SmartThings Find network), and affordability. With a price point of just $29.99 for the SmartTag, and $39.99 for the SmartTag+ with more advanced tracking capabilities, the SmartTags have become a weapon of choice of stalkers and abusers.

---

[3] *Id.*

[4] Blaauw, E., Arensman, E., Winkel, F.W., Freeve, A., & Sheridan, L. (2002). The Toll of Stalking. Journal of Interpersonal Violence 17(1): 50-63 (available at: https://journals.sagepub.com/doi/10.1177/0886260502017001004).

8. The SmartTags work by emitting signals that are detected by Bluetooth sensors on the hundreds of millions of Samsung products across the United States. These sensors comprise Samsung's "SmartThings" network. When a device on the network detects a signal from the missing device, it reports that missing device's location back to Samsung, which in turn reports it to the owner.

9. The ubiquity of Samsung products, and their constituency in the Galaxy SmartThings Find network, means that a SmartTag can more reliably transmit location data than competitors.

10. None of this came as a surprise to Samsung. Prior to and upon the SmartTag's release, advocates and technologists urged the company to rethink the product and to consider its inevitable use in stalking. In response, Samsung heedlessly forged ahead, dismissing concerns and pointing to mitigation features that it claimed rendered the devices safe.

11. The concerns were well founded. Immediately after the SmartTag's release, and consistently since, reports have proliferated of people finding SmartTags placed in their purses, in or on their cars, and even sewn into the lining of their clothes, by stalkers in order to track their whereabouts.

12. Plaintiff, a victim of stalking through the use of a Samsung SmartTag, brings this action on behalf of herself and a class and subclasses of individuals who have been and who are at risk of stalking via this dangerous product.

13. Samsung's acts and practices, as detailed further herein, amount to acts of negligence, negligence per se, intrusion-upon-seclusion, and product liability, and constitute unjust enrichment. Plaintiff, in a representative capacity, seeks actual damages, and punitive damages, as well as injunctive and declaratory relief against Samsung, correcting Samsung's practice of

releasing an unreasonably dangerous product into the stream of commerce, misrepresenting the harms associated therewith, and facilitating the unwanted and unconsented to location tracking of Plaintiff and Class members.

PARTIES

14. Plaintiff Jane Doe is a citizen of Philadelphia County, Pennsylvania. Ms. Doe was stalked for over a year, using a Samsung SmartTag.

15. Defendant Samsung Electronics Co., Ltd. ("SECL") is one of the world's largest producers of electronics and electronic devices. SECL is a multinational corporation existing under the laws of the Republic of South Korea, and headquartered at 129 Samsung-ro, Yeongtong-gu Suwon, Gyeonggi, 16677, Republic of Korea, and is the parent company to Defendant Samsung Electronics America, Inc.

16. SECL regularly conducts business in the Commonwealth of Pennsylvania and throughout the United States. SECL's primary consumer products are smartphones, tablets, laptop computers, and televisions. SECL generally oversees all aspects of these products, including but not limited to their design, manufacture, marketing, and warranty services.

17. Defendant Samsung Electronics America, Inc. ("SEAI"; or together with SECL, "Samsung" or "Defendants") is a wholly owned subsidiary of SECL. SEAI is a New York corporation, headquartered at 85 Challenger Rd., 6th Floor, Ridgefield Park, NJ 07660.

JURISDICTION AND VENUE

18. Pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005 ("CAFA"), this Court has subject matter jurisdiction over this putative nationwide class action because the matter in controversy exceeds $5,000,000.00, exclusive of interest and costs, and is a

class action in which some members of the Class are citizens of states different than Defendant. See 28 U.S.C. § 1332(d)(2)(A).

19. This Court has personal jurisdiction over Defendant because it conducts substantial business in Pennsylvania, from which the claims in this case arise.

20. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(b)(1) because a substantial part of the events or omissions which give rise to the claims alleged herein occurred in in this district.

FACTUAL ALLEGATIONS

Samsung Galaxy SmartTags, Generally

21. The Samsung SmartTag was introduced in January 2021 as a standalone product. Roughly the size of a US half-dollar, it is a tracking beacon, meant to help customers locate other objects, such as keys, a bag, or a car.[5]

Fig 1.

22. On April 16, 2021, Samsung released the Galaxy SmartTag+, an upgraded version equipped with both Bluetooth Low Energy (BLE) and ultra-wideband (UWB) technology which

[5] https://news.samsung.com/global/introducing-the-new-galaxy-smarttagplus-the-smart-way-to-find-lost-items

offers short-range location tracking, making it possible to pinpoint the location of the device with greater accuracy.[6]

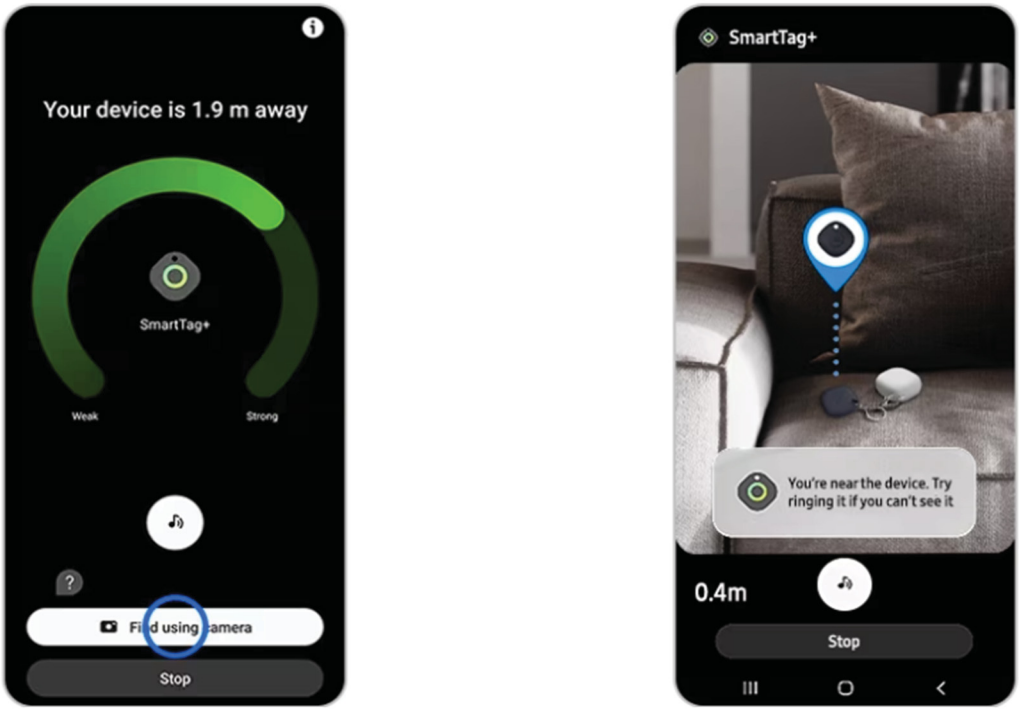


Fig. 2

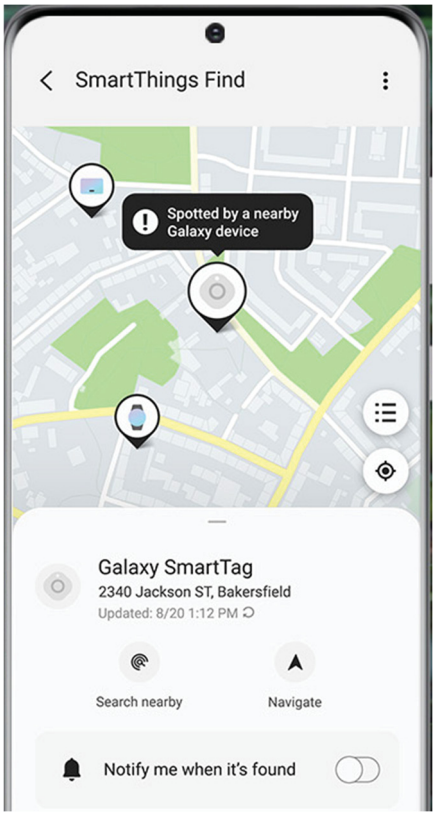
23. SmartTags are not themselves connected to the Internet. Instead, they utilize Bluetooth technology, emitting Bluetooth signals to a Samsung Galaxy mobile device that is nearby. In turn, those devices report where a SmartTag has last been seen.

24. More than 70 million devices were registered to the SmartThings Find network within the first six months of its launch in October 2020. On May 3, 2023, Samsung announced

[6] Samsung Newsroom, Apr. 8, 2021 (available at: https://news.samsung.com/global/introducing-the-new-galaxy-smarttagplus-the-smart-way-to-find-lost-items).

that SmartThings Find has expanded to over 300 million registered and opted-in devices that can be used to identify SmartTags locations.[7]

25. Once a SmartTag is identified as being near a Samsung Galaxy device or multiple Samsung Galaxy devices, the devices act as crowdsourced beacons, or "find nodes," pinging the SmartTag to locate it for the SmartTag owner's sake. These devices receive the signal from a SmartTag and send the location to the SmartThings server, allowing the SmartTag owner to find the SmartTag, "no matter how far away it is."[8]



[7] Samsung Newsroom, May 11, 2023 (available at: https://www.samsungmobilepress.com/press-releases/samsung-smartthings-find-rapidly-expands-with-over-300-million-nodes-helping-to-locate-devices).

[8] Samsung, "How can I join the Galaxy Find Network?, May 17, 2021 (available at: https://www.samsung.com/ae/support/mobile-devices/how-can-i-join-the-galaxy-find-network/#:~:text=The%20Galaxy%20Find%20network%20is,how%20far%20away%20it%20is)

Fig. 3

26. Once a Samsung Galaxy device recognizes the connected SmartTag, the owner sees the SmartTag's location on a map, as well as a record of the dates and times the device was at a given location.[9]

27. Bluetooth range is approximately 30 feet. Thus, for a SmartTag to be identified by a device, it must come within 30 feet of a linked device, at which time, the SmartTag will have been located on Samsung's network of Galaxy tablets, phones, and other mobile devices in the SmartThings Find network. This network is vast: as of 2023, Samsung holds 28.52% of the smartphone market share in the United States.[10]

28. Samsung Sought to Dismiss and Minimize Concerns About the Threats Surrounding SmartTags following the release of the SmartTag+. On April 20, 2021, three months after the SmartTag's launch, Samsung introduced the "SmartThings Find" feature into its SmartThings application on the Android operating system architecture.[11] According to Samsung, SmartThings Find would allow customers to "ensure nobody is secretly tracking," their location.[12]

[9] Samsung.com, Samsung Galaxy SmartTag, product page (available at: https://www.samsung.com/us/mobile/mobile-accessories/phones/samsung-galaxy-smart-tag-1-pack-black-ei-t5300bbegus/).

[10] https://www.bankmycell.com/blog/us-smartphone-market-share

[11] Mehrotra, P. XDA Developers, Apr 20, 2021 (available at: https://www.xda-developers.com/samsungs-smartthings-find-scan-unknown-galaxy-smart-tags/).

[12] Samsung Newsroom, "Evolving for the Better: SmartThings Ecosystem Gives Galaxy Users Better Control Over Their Connected Devices," Apr 20, 2021 (available at: https://news.samsung.com/global/evolving-for-the-better-smartthings-ecosystem-gives-galaxy-users-better-control-over-their-connected-devices).

Individuals Have Few, If Any, Meaningful Resources When They Are Tracked

29. While Samsung has built safeguards into the Samsung product, they are woefully inadequate, and do little, if anything, to promptly warn individuals if they are being tracked. Moreover, there is a gross imbalance between the protections available to Samsung/Android users versus those available to individuals with iOS/Apple devices—rendering iOS/Apple users nearly defenseless to tracking/stalking using a SmartTag.

30. The SmartThings Find feature does little to eliminate the dangers of stalking, as even Samsung users need to be acquainted with the SmartThings Find app, have the latest version installed, and need to actively scan themselves, with no proactive notification from the device or SmartThings app, that the individual may be tracked. Individuals with Samsung phones will find that the SmartThings App comes pre-installed, however the individual needs to take steps to set up the SmartThings Find feature. First, a Samsung user needs to downloaded necessary "add-ons" to allow the SmartThings Find feature to work.[13]

31. Users of mobile devices running the Android operating system on a non-Samsung device likewise need to take multiple proactive steps in order to access the SmartThings Find feature. First, a non-Samsung Android user must verify that their device is running the Android 8.0 or later operating system. If so, the Android user must download the SmartThings app from the Google Play store, set the app to use the device's location information, and then actively initiate the feature to scan the nearby area for unknown and potentially unwanted SmartTags travelling in close proximity.

[13] Maring, J., "How to use SmartThings Find on a Samsung Phone" (available at: https://www.androidcentral.com/how-use-smartthings-find-samsung-phone).

32. While a user of a Samsung Galaxy or similar Android phone owner might be able to trigger an alert that then makes them aware of the potential danger of being tracked by a SmartTag, users of iOS phones and devices do not have that protection, as their devices run on the iOS operating system, which is outside of the control of Samsung. While the SmartThings app is available for iOS devices, the SmartThings Find feature that allows users to initiate an Uknown Tag Search is not available.[14] To date, Samsung has not worked in conjunction with Apple to provide automated alerts when iOS users are being stalked.

33. Thus, individuals who own iPhones, iPads, or iPod Touches are more vulnerable to being tracked using a SmartTag. iOS mobile devices have a 59.64% market share in the United States,[15] meaning that over half of America's population would not receive any notification if they were being stalked by a SmartTag.

34. Samsung's efforts to mitigate the dangers of the SmartTag product fall woefully short. The lack of reliable security features has caused individuals to be vulnerable to stalking.

35. As an example of the dangers of the SmartTag, on May 31, 2022, Geoffrey Fowler, the prominent tech reporter for the Washington Post, published a story in which he detailed his use of a Samsung SmartTag to "mirror[] how a stalker might use tracker tags to follow his victim." He did this by slipping a SmartTag linked to a test phone, into his baby's stroller, then went for a walk using a different iPhone and Android phone unknown to the SmartTag.

[14] Fowler, Geoffrey A. "Am I being tracked? Anti-stalking tech from Apple, Tile falls short," Mar. 31, 2022 (available at: https://www.washingtonpost.com/technology/2022/03/31/airtags-stalking/).

[15] Statcounter Global Stats, "Mobile Operating System Market Share United States Of America Apr 2022 - Apr 2023" (available at: https://gs.statcounter.com/os-market-share/mobile/united-states-of-america).

36. Fowler cautioned that, even with the SmartThings Find function enabled (which he describes as difficult in the below) he was able to complete a long walk without once being notified that an unknown SmartTag was traveling with him:

> Samsung's SmartTag detector [SmartThings Find] is buried so deeply in the settings of its SmartThings app, I had to ask the company where to find it. Then on my first stroll, the app failed to find my test SmartTag. Later, Samsung told me that its software wouldn't identify a tag until it had been separated from the phone that owned it for a full 24 hours. (How does this make sense, if domestic violence victims live with their stalkers?) Worse, Samsung's software doesn't work on iOS, so I never located the SmartTag with my test iPhone.

Victims of Stalking Via SmartTags Have Little Meaningful Recourse

37. Even if a victim of SmartTag stalking is able to discover the SmartTag and bring it to law enforcement, there are very few, meaningful protections that such a victim would then be able to receive. At present, only 23 states have electronic tracking laws,[16] and stalking, in and of itself, is a crime that often goes unprosecuted:

> Stalking goes unrecognized, uncharged, and unprosecuted for a number of reasons. Victims, police, and prosecutors often fail to recognize patterns of behavior as "stalking," or associate the term exclusively with following, monitoring, or surveillance--acts that represent only one variety of the many types of behavior that may fit the statutory definition of stalking. Police and prosecutors may focus on a specific incident that resulted in a law enforcement response (e.g., an assault, an isolated threat, an act of vandalism) and fail to explore the context within which the act was committed—context that may include a course of conduct chargeable as stalking. Prosecutors, failing to understand the strategic value of a stalking charge, may wonder why they should bother "complicating" their

[16] Alexis McAdams, "Apple AirTags, meant to help you track your stuff, have become tools of stalkers and criminals," Fox News (June 14, 2022) (available at https://www.foxnews.com/tech/Apple-airtag-stalking-dangerous-crime).

> case when they have strong evidence of a crime that is perceived to be more serious and easier to prosecute.[17]

38. Indeed, the number of individuals who are stalked in the United States is jaw dropping. More than 6 million people over the age of 18 are stalked each year in the United States, according to data from the Department of Justice's Bureau of Justice Statistics (BJS).[18] That number is believed to be much higher, however, as BJS statistics indicate just 40% of stalking cases are reported to police.[19] According to the Stalking Prevention, Awareness, and Resource Center (SPARC), one in six women and one in 17 men are stalking survivors. Roughly 15% of those individuals said the stalking forced them to move.[53] Yet, once reported to the police, only 8% of stalking perpetrators are arrested.[54]

The Federal Trade Commission Makes Clear That Stalking Technologies and Unwanted Location Tracking Violates Section 5 of the FTC Act

39. Recent enforcement actions by the FTC directly speak to the plainly-illegal, dangerous, and fundamentally unfair nature of Samsung's conduct.

40. For example, in August 2022, the Commission filed suit against the data broker Kochava, Inc.:

> F]or selling geolocation data from hundreds of millions of mobile devices that can be used to trace the movements of individuals to and from sensitive locations. Kochava's data can reveal people's visits to reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities. The FTC alleges that by selling data tracking people, Kochava is

---

[17] Stalking Prevention Awareness and Resource Center ("SPARC"). Prosecutor's Guide to Stalking (2020) (available at https://www.stalkingawareness.org/wp-content/uploads/2020/01/SPA-19.005-Prosecutors-Guide-to-Stalking-00000002.pdf).

[18] Megan Stone, "After 9-year fight to prosecute her stalker, woman shares story to help other survivors," ABC News (Jan. 5, 2021) (available at https://abcnews.go.com/GMA/Living/year-fight-prosecute-stalker-woman-shares-story-survivors/story?id=74878256).

[19] *Id.*

> enabling others to identify individuals and exposing them to threats of stigma, stalking, discrimination, job loss, and even physical violence.[20]

41. Per the Commission, the lawsuit involves Kochava's "vast troves of location information derived from hundreds of millions of mobile devices….People are often unaware that their location data is being purchased and shared by Kochava and have no control over its sale or use."[21]

42. Risks associated with the unwanted collection of location data include identification of individuals' home addresses, and, more broadly, "puts consumers at significant risk. The company's data allows purchasers to track people at sensitive locations that could reveal information about their personal health decisions, religious beliefs, and steps they are taking to protect themselves from abusers. The release of this data could expose them to stigma, discrimination, physical violence, emotional distress, and other harms."[22]

43. Such acts and practices "reveal consumers' visits to sensitive locations, including, among others, locations associated with medical care, reproductive health, religious worship, mental health, temporary shelters, such as shelters for the homeless, domestic violence survivors, or other at-risk populations, and addiction recovery" and, in turn "cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not

---

[20] Federal Trade Commission, "FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations" (August 29, 2022) (available at https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other).

[21] *Id.*

[22] *Id.*

outweighed by countervailing benefits to consumers or competition." Accordingly, they "constitute unfair acts or practices in violation of Section 5 of the FTC Act."[23]

44. The enforcement action against Kochava is not an outlier. In 2019, the FTC brought an enforcement action against Retina-X, a company accused of creating "stalking apps," that could be placed on users phones in order to surreptitiously surveil them. Like the Kochava action, and like the instant action against Samsung, "these apps were designed to run surreptitiously in the background and are uniquely suited to illegal and dangerous uses. Under these circumstances, we will seek to hold app developers accountable for designing and marketing a dangerous product."[24]

45. There, as here, the defendant "sold monitoring products and services that required circumventing certain security protections implemented by the Mobile Device operating system or manufacturer, and did so without taking reasonable steps to ensure that the monitoring products and services will be used only for legitimate and lawful purposes by the purchaser. Respondents' actions cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. This practice is an unfair act or practice [in violation of the FTA Act]."[25]

---

[23] Complaint, *Federal Trade Commission v. Kochava, Inc.*, Case No. 2:22-cv-377 (D. Idaho), Dkt. No. 1 at ¶¶ 36-38.

[24] Federal Trade Commission, "*FTC Brings First Case Against Developers of 'Stalking' Apps*," (October 22, 2019) (available at: https://www.ftc.gov/news-events/news/press-releases/2019/10/ftc-brings-first-case-against-developers-stalking-apps).

[25] *In the Matter of Retina-X Studios, LLC, a limited liability company; and James N. Johns, Jr., individually and as sole member of Retina-X Studios, LLC.*, FTC Matter/File Number 172-3118, Complaint, at ¶ 32.

Plaintiff's Experience with SmartTags

46. Plaintiff Jane Doe is the victim of stalking by her ex-boyfriend using a Samsung SmartTag. Upon information and belief, this period of stalking began on or about November 2021, when Ms. Doe was still in a relationship with her ex-boyfriend, and continued until the tracking device was ultimately discovered on or about September 2022.

47. Ms. Doe first became suspicious that she was being tracked in April of 2022. During a separation period between Plaintiff and her stalker, she received a disturbing message from her ex which indicated that he "had eyes on her" and was aware of her location.

48. During a brief conciliation with her ex, Ms. Doe noticed something that gave her pause: Her then partner's phone was alerting him that a tracking device was nearby. Her suspicions were further heightened in July of 2022, when Ms. Doe discovered airline tickets that indicated that her ex was traveling during the period in or around April 2022 when he indicated he knew her location – making it impossible that he would have known where she was without use of a tracking device.

49. While her ex initially denied that he was tracking Ms. Doe's location, upon persistent questioning, he came clean and admitted that he did in fact have a tracker on Plaintiff, but that he had removed it.

50. In August of 2022, Ms. Doe and her stalker permanently ended their relationship. However, Ms. Doe's suspicion that she was being tracked persisted.

51. Soon after, Ms. Doe acquired two apps: "Tracker Detect" and "Air Guard," which, allow users to determine the existence of nearby tracking devices. Despite her suspicions, the apps did not locate any tracking devices in the vicinity of Ms. Doe's vehicle.

52. This sense of relief would not last. On or about September 2nd Ms. Doe again received a message from her ex indicating that he was aware of her location. Ms. Doe went to the police to file a report and request help searching her vehicle for a tracking device. Unfortunately, the police were unable to locate the tracker and instead urged her to file a restraining order.

53. Based on her conversation with her ex and the ineffectiveness of the tracker detection apps which were catered to locate Apple AirTags, Ms. Doe deduced that the device her stalker was using was a Samsung SmartTag.

54. That evening, Ms. Doe reached out to Samsung for assistance in locating the device her ex was utilizing to track her location. Samsung offered no assistance. Pursuing an alternate route, Ms. Doe was able to convince her ex to admit the location of the Samsung SmartTag.

55. Ms. Doe confronted her ex about whether the tracker was still connected to her vehicle. After some back-and-forth, he admitted that it was on rear bumper of her car.

56. Ms. Doe returned to her vehicle and found it attached with double sided tape to the bottom of her back bumper.

57. Between September 3rd and September 24th, Ms. Doe repeatedly called Samsung with help in locating additional tracking devices, and repeatedly Samsung demurred in assisting her.

58. On or about September 24th, 2022 Ms. Doe finally reached a customer service agent who did personal research on Ms. Doe's behalf. This can be seen through a text-message thread where Ms. Doe sent over articles from third-party news organizations that indicated that the Samsung SmartTag was, in fact, locatable if it is placed on your person.

59. Only after this collaboration was the agent able to guide Ms. Doe through the process of downloading Samsung's own "Smart Things" app, which has the ability to locate nearby

Samsung tracking devices. Revealing this functionality was demonstrably an *ultra vires* act of goodwill on behalf of the agent, as evidenced by the numerous customer service calls Ms. Doe had made prior that resulted in no help in locating additional devices.

CLASS ALLEGATIONS

60. Plaintiff brings this class action, pursuant to Rule 23 of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes and sub-classes, which are jointly referred to throughout this Complaint as the "Class:"

> **The Stalked Class:** all persons residing in the United States who were tracked, without consent, by Samsung's SmartTag.
>
> **The At-Risk-Of-Stalking Class:** all persons residing in the United States who own iOS or Android devices.
>
> **The Multistate Sub-Class:** all persons residing in the States of Alabama, Alaska, Arizona, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Minnesota, Missouri, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, South Dakota, Texas, Utah, Vermont, Washington, and West Virginia who were tracked, without consent, by Samsung's SmartTags.

61. Plaintiff Jane Doe is the proposed Class Representative for the Stalked Class and the At-Risk-Of-Stalking Class, as well as the Multi-State Subclass.

62. Excluded from each Class are the following individuals: officers and directors of Samsung and its parents, subsidiaries, affiliates, and any entity in which Samsung has a controlling interest; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

63. Plaintiff reserves the right to modify or amend the definition of each of the proposed Classes before the Court determines whether certification is appropriate.

64. This action readily satisfies the requirements set forth under Federal Rule of Civil Procedure 23:

a. Each Class is so numerous that joinder of all members is impracticable.

b. There are questions of law or fact common to the Classes. These questions include, but are not limited to, the following:

i. Whether Samsung's acts and practices complained of herein amount to the use of an electronic tracking device to determine the location or movement of a person;

ii. Whether Samsung's acts and practices complained of herein amount to egregious breaches of social norms;

iii. Whether Samsung acted intentionally in violating Plaintiff's and Class members' privacy rights;

iv. Whether an injunction should issue; and

v. Whether declaratory relief should be granted.

c. Plaintiff's claims are typical of the claims of the Class in that Plaintiff, like all Class members, was subjected to unwanted stalking via Samsung SmartTag.

d. Moreover, like all Class Members, Plaintiff suffers a substantial risk of repeated injury in the future. Plaintiff continues to be at risk of unwanted and unlawful tracking via a SmartTag device. Because the conduct complained of herein is systemic, Plaintiff and all Class Members face substantial risk of the same injury in the future. Samsung's conduct is common to all Class members and represents a common pattern of conduct resulting in injury to all members of the Class. Plaintiff has suffered the harm alleged and has no interests antagonistic to any other Class member.

e. Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff's interests do not conflict with the interests of the Class members. Furthermore, Plaintiff has retained competent counsel experienced in class action litigation, consumer protection litigation, and electronic privacy litigation. Plaintiff's counsel will fairly and adequately protect and represent the interests of the Class. FRCP 23(a)(4) and 23(g) are satisfied.

f. In acting as above-alleged, and in failing and refusing to cease and desist despite public outcry, Samsung has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and corresponding declaratory relief each appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual Class members that would establish incompatible standards of conduct for Samsung.

g. Injunctive relief is necessary to prevent further unlawful and unfair conduct by Samsung. Money damages, alone, could not afford adequate and complete relief, and injunctive relief is necessary to restrain Samsung from continuing to commit its illegal and unfair violations of privacy.

CAUSES OF ACTION

COUNT I
(Negligence)
(On Behalf of the Class)

65. Plaintiff repeats and realleges all preceding paragraphs contained herein. Samsung owed Plaintiff and Class members a duty of care in its design, marketing, and introduction into the market of its SmartTags. This duty is evidenced by, *inter alia*, Samsung's unique position to monitor Plaintiff's and Class members' behavior through SmartTags' access to Samsung's vast network of mobile devices, which in turn are used to locate Plaintiff and Class members with

unparalleled reach and precision. It is further supported by the surreptitious and non-intuitive nature of Defendant's tracking.

66. Samsung breached that duty by rushing SmartTags to market with insufficient safeguards to prohibit their use for stalking purposes.

67. This breach of duty on the part of Samsung was the proximate or legal cause of injury suffered by Plaintiff and Class members.

68. As a result of Samsung's actions, Plaintiff and Class members seek injunctive relief, damages, and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Samsung's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights. Punitive damages are warranted to deter Samsung from engaging in future misconduct.

COUNT II
(Strict Liability – Design Defect – Consumer Expectation Test)
(On Behalf of the Class)

69. Plaintiff repeats and realleges all preceding paragraphs contained herein.

70. Samsung designed, developed and programmed its Galaxy SmartTags products.

71. Samsung, by and through its employees, agents, subsidiaries and/or successor corportations are strictly liable under § 402A of the Restatement (Second) of Torts by:

a. Designing, developing, manufacturing, selling and/or distributing a defective product in a defective condition;

b. Designing, developing, manufacturing, selling and/or distributing a product without adequate warnings

c. Designing, developing, manufacturing, selling and/or distributing a product without adequate or necessary safeguards to prevent the product from being used to stalk or otherwise harm others;

d. Designing, developing, manufacturing, selling and/or distributing a product for which the ricks of use far outweigh the utility thereof;[26]

e. Designing, developing, manufacturing, selling and/or distributing product that was unreasonably dangerous for its intended and forseeable uses and/or misuses and to its intended and forseeable victims, such as Plaintiff;

f. Designing, developing, manufacturing, selling and/or distributing a product that laced the necessary safety features to prevent harm to Plaintiff and others;

g. Failing to warn the public of the risks associated with its product;

72. Samsung manufactures, distributes, and sells its Galaxy SmartTags products.

73. The foreseeability of the use/misuse of SmartTags for stalking is evidenced by, *inter alia*, the fact that Samsung preemptively sought to assuage consumer fears by (falsely) claiming that the SmartTags Find feature would "ensure nobody is secretly tracking your location," in a press release.[27]

74. Plaintiff and Class members were harmed as a result of the SmartTag's design defect.

75. The SmartTag's design defect was a substantial factor in causing Plaintiff's and Class members' harm.

[26] A consideration of the following factors—the gravity of the potential harm caused by the design defect (i.e., its propensity for use in stalking and other crimes); the likelihood that this harm would occur; the feasibility of an alternative safer design at the time of manufacture; the cost of an alternative design; and any disadvantages of an alternative design all weigh in favor of Plaintiff and the Class, and make clear that the risks associated with the SmartTags outweigh the benefits

[27] *Supra*, Note 12.

76. As a result of Samsung's actions, Plaintiff and Class members seek injunctive relief, damages, and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Samsung's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights. Punitive damages are warranted to deter Samsung from engaging in future misconduct.

COUNT III
(Unjust Enrichment)
(On Behalf of the Class)

77. Plaintiff repeats and realleges all preceding paragraphs contained herein.

78. Samsung should not have released the SmartTag into the stream of commerce, because of the dangers detailed herein.

79. As a result of Samsung's selling the SmartTag, Samsung received a benefit, which it is unjust for Samsung to retain.

80. Under the circumstances, it is against equity and good conscience to permit Samsung to retain the ill-gotten benefits that it received from the conduct complained of herein.

81. As a direct and proximate result of Samsung's actions, Samsung has been unjustly enriched. Plaintiff and Class members have a right to restitution in an amount to be proven at trial.

COUNT IV
(Intrusion Upon Seclusion)
(On Behalf of the Class)

82. Plaintiff repeats and realleges all preceding paragraphs contained herein.

83. Plaintiff and Class members have reasonable expectations of privacy in their persons and their whereabouts, generally. Plaintiff's and Class members' private affairs include their locations.

84. The reasonableness of such expectations of privacy is supported by Samsung's unique position to monitor Plaintiff's and Class members' behavior through SmartTags' access to Samsung's vast network of mobile devices, which in turn are used to locate Plaintiff and Class members with unparalleled reach and precision. It is further supported by the surreptitious and non-intuitive nature of Defendant's tracking.

85. Defendant intentionally intruded on and into Plaintiff's and Class members' solitude, seclusion, or private affairs by intentionally geolocating them.

86. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, Supreme Court precedent (most recently and forcefully articulated in the *Carpenter* opinion), legislation enacted by Congress, rules promulgated and enforcement actions undertaken by the FTC, and countless studies, op-eds, and articles decrying location tracking, particularly in the context of stalking and abuse.

87. Plaintiff and Class members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

88. Samsung's actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class members.

89. As a result of Samsung's actions, Plaintiff and Class members seek injunctive relief, damages, and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Samsung's actions—which were malicious, oppressive, and willful—were calculated to injure Plaintiff and Class members and made in conscious disregard of Plaintiff's and Class members' rights. Punitive damages are warranted to deter Samsung from engaging in future misconduct.

RELIEF REQUESTED

90. Plaintiff, on behalf of herself and members of the general public, requests that the Court enter judgment against Defendant, and accordingly, request the following:

a. That judgment be entered against Defendant and in favor of Plaintiff on the causes of action set forth in this Complaint;

b. That judgment be entered against Defendant for all injunctive, declaratory, and other equitable relief sought, including but not limited to an order enjoining Samsung from further unlawful, unfair and/or fraudulent practices with respect to the design, manufacture, and release into the market of its SmartTags;

c. That Plaintiff and Class members be awarded actual, nominal, and/or punitive damages, in an amount to be determined at trial;

d. Reasonable attorney's fees and litigation costs; and

e. All other such other relief as may be appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a jury trial on all triable issues.

Dated: October 16, 2023

Respectfully submitted,

/s/ Edwin J. Kilpela, Jr.

Edwin J. Kilpela, Jr.
PA ID # 201595
Elizabeth Pollock-Avery
PA ID# 314841
LYNCH CARPENTER, LLP
1133 Penn Ave, 5th Floor
Pittsburgh, Pennsylvania 15222
Tel: (412) 322-9243
Fax: (412) 231-0246
ekilpela@lcllp.com
elizabeth@lcllp.com

MILSTEIN JACKSON FAIRCHILD & WADE, LLP
Gillian L. Wade
Sara D. Avila
Marc A. Castaneda
10990 Wilshire Blvd., 8th Floor
Los Angeles, California 90024
Tel: (310) 396-9600
Fax: (310) 396-9635
gwade@mjfwlaw.com
savila@mjfwlaw.com
mcastaneda@mjfwlaw.com

wh LAW
David Slade
Brandon Haubert
Jessica Hall
1 Riverfront Place, Suite 745
North Little Rock, AR 72114
Telephone: 501.891.6000
Facsimile: 501.222.3027
slade@wh.law
brandon@wh.law
jessica@wh.law

Attorneys for Plaintiff